

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-005641
 (43)Date of publication of application : 08.01.2003

(51)Int.Cl. G09C 1/00
 H04L 9/08
 H04L 12/28

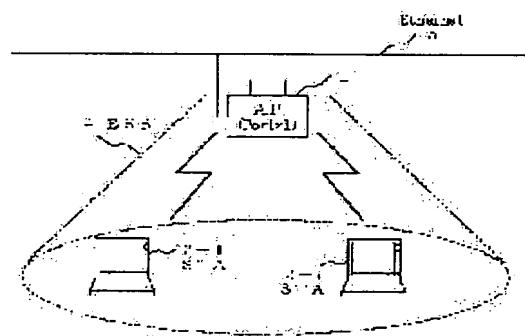
(21)Application number : 2001-191559 (71)Applicant : NEC CORP
 (22)Date of filing : 25.06.2001 (72)Inventor : SHIMIZU MEGUMI

(54) METHOD AND APPARATUS FOR AUTHENTICATION IN WIRELESS LAN SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and an apparatus for authentication in a wireless LAN system which can concurrently achieve delivery of an encryption key for maintaining concealment between only parties performing wireless communication and an authenticating procedure and can simplify each authenticating procedure to the same AP (a base station) performed by a STA (a mobile terminal) completing initial authentication after releasing the authentication.

SOLUTION: The STA searches whether a MAC address of the AP intending to perform the wireless communication exists in an AP information managing table maintained by the STA. If the MAC address does not exist in the AP information managing table, a request for authenticating a public key is transmitted to the AP. If the MAC address exists in the AP information managing table, a request for re-authenticating the public key is transmitted to the AP.



LEGAL STATUS

[Date of request for examination]	28.05.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3702812
[Date of registration]	29.07.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-5641

(P2003-5641A)

(43)公開日 平成15年1月8日(2003.1.8)

(51)Int.Cl. ⁷	識別記号	F I	テマコード*(参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 12/28	3 0 0 Z 5 K 0 3 3
12/28	3 0 0	9/00	6 0 1 C
			6 0 1 E

審査請求 有 請求項の数16 O.L (全 13 頁)

(21)出願番号 特願2001-191559(P2001-191559)

(22)出願日 平成13年6月25日(2001.6.25)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 清水 めぐみ

東京都港区芝五丁目7番1号 日本電気株
式会社内

(74)代理人 100082935

弁理士 京本 直樹 (外2名)

Fターム(参考) 5J104 AA07 AA16 EA06 EA19 KA02

KA05 KA06 NA02 NA20

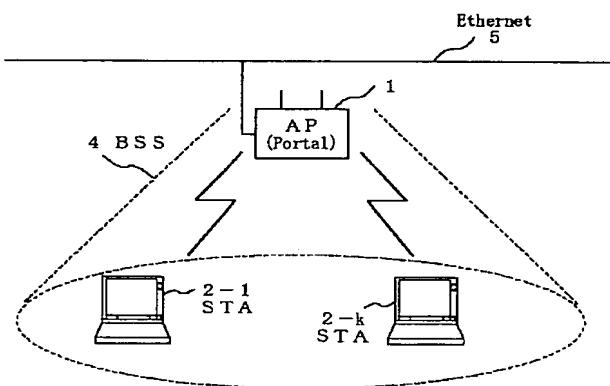
5K033 AA08 CC02 DA01 DA19

(54)【発明の名称】 無線LANシステムにおける認証方法と認証装置

(57)【要約】

【課題】無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配達と認証手順の同時実現を可能とすると共に、初回の認証を完了したSTA(移動端末局)に関しては、認証解除後の同一AP(基地局)に対する2回目以降の認証手順の簡略化を実現可能とする、無線LANシステムにおける認証方法と認証装置を提供する。

【解決手段】STAは、無線通信を行おうとするAPのMACアドレスがSTAの保持するAP情報管理テーブル内に存在するか否かを検索し、前記MACアドレスが前記AP情報管理テーブル内に存在しない場合には、前記APに対して公開鍵認証要求を行い、前記MACアドレスが前記AP情報管理テーブル内に存在する場合には、前記APに対して公開鍵再認証要求を行うことを特徴とする。



【特許請求の範囲】

【請求項 1】 無線 LAN システムにおける認証方法において、STA (移動端末局) は、無線通信を行おうとする AP (基地局) の MAC アドレスが前記 STA の保持する AP 情報管理テーブル内に存在するか否かを検索し、前記 MAC アドレスが前記 AP 情報管理テーブル内に存在しない場合には、前記 STA は前記 AP に対して公開鍵認証要求を行い、前記 AP は前記公開鍵認証要求が妥当である場合には前記 STA の認証を行い、前記 MAC アドレスが前記 AP 情報管理テーブル内に存在する場合には、前記 STA は前記 AP に対して公開鍵再認証要求を行い、前記 AP は前記公開鍵再認証要求が妥当である場合には前記 STA の認証を行う、ことを特徴とする無線 LAN システムにおける認証方法。

【請求項 2】 前記 AP 情報管理テーブルは、前記 STA が前記公開鍵認証要求を行って該公開鍵認証の完了実績の有る AP の MAC アドレスを最新認証完了実績順に保持することを特徴とする請求項 1 に記載の無線 LAN システムにおける認証方法。

【請求項 3】 前記 AP は、自らの秘密鍵である AP 秘密鍵と、前記 AP 秘密鍵に対応する公開鍵であるところの AP 公開鍵と、前記 AP 公開鍵を付した自らのユーザ証明書であるところの AP ユーザ証明書とを保持し、前記 STA は、自らの秘密鍵である STA 秘密鍵と、前記 STA 秘密鍵に対応する公開鍵であるところの STA 公開鍵と、前記 STA 公開鍵を付した自らのユーザ証明書であるところの STA ユーザ証明書とを保持している、ことを特徴とする請求項 1 或いは請求項 2 の何れか 1 項に記載の無線 LAN システムにおける認証方法。

【請求項 4】 前記 STA が前記 AP に対して前記公開鍵認証要求を行うステップは、公開鍵認証手順によって構成され、前記公開鍵認証手順は、前記 STA から前記 AP に対して認証要求を行うステップと、前記認証要求を受信した前記 AP から前記 STA に対して前記 AP ユーザ証明書を送信するステップと、前記 AP ユーザ証明書を受信した前記 STA が、前記 AP ユーザ証明書を検証した後に前記 AP ユーザ証明書に添付された前記 AP 公開鍵を用いて前記 STA ユーザ証明書を暗号化して暗号化 STA ユーザ証明書を作成し、前記暗号化 STA ユーザ証明書を前記 AP に対して送信するステップと、前記暗号化 STA ユーザ証明書を受信した前記 AP が、前記暗号化 STA ユーザ証明書を前記 AP 秘密鍵で復号化して前記 STA ユーザ証明書を再生し、前記 STA ユーザ証明書を検証した後に前記 STA ユーザ証明書に添付された前記 STA 公開鍵を用いて前記 AP が生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記 STA に送信して認証許可を通知するステップとから構成され、前記暗号化共通鍵を受信した前記 STA が、前記暗号化共通鍵を前記 STA 秘密鍵で復号化して前記 STA 共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする請求項 6 に記載の無線 LAN システムにおける認証方法。

【請求項 5】 前記 STA が前記 AP に対して前記公開鍵再認証要求を行う際に送受信される MAC フレーム内のフレームボディ部のAlgorithm Number の値は、「0」又は「1」でない任意の数「n」である、ことを特徴とする請求項 4 に記載の無線 LAN システムにおける認証方法。

【請求項 6】 前記 AP は公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記 AP が過去に認証許可を通知した実績の有る前記 STA の MAC アドレスと、該 STA の前記 STA 公開鍵と、前記 AP が該 STA の認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする請求項 5 に記載の無線 LAN システムにおける認証方法。

【請求項 7】 前記 STA が前記 AP に対して前記公開鍵再認証要求を行なうステップは、公開鍵再認証手順によつて構成され、前記公開鍵再認証手順は、前記 STA から前記 AP に対して再認証要求を行なうステップと、前記再認証要求を受信した前記 AP が、前記公開鍵再認証要求を送信した前記 STA の MAC アドレスが前記 AP の保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記 STA の MAC アドレスが前記公開鍵管理テーブルに存在し、かつ、該 MAC アドレスに対応する公開鍵であるところの前記 STA 公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記 AP は、当該 STA に対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記 STA 公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記 STA に送信して認証許可を通知するステップとから構成され、前記暗号化新共通鍵を受信した前記 STA が、前記暗号化新共通鍵を前記 STA 秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする請求項 6 に記載の無線 LAN システムにおける認証方法。

【請求項 8】 前記 STA が前記 AP に対して前記公開鍵再認証要求を行なう際に送受信される MAC フレーム内のフレームボディ部のAlgorithm Number の値は、「0」と「1」と「n」でない任意の数「m」である、ことを特徴とする請求項 7 に記載の無線 LAN システムにおける認証方法。

【請求項 9】 無線 LAN システムにおける認証装置において、無線通信を行おうとする AP (基地局) の MAC アドレスが自身の保持する AP 情報管理テーブル内に存在するか否かを検索し、前記 MAC アドレスが前記 AP 情報管理テーブル内に存在しない場合には、前記 AP に対して公開鍵認証要求を行い、前記 MAC アドレスが前記 AP 情報管理テーブル内に存在する場合には、前記 AP に対して公開鍵再認証要求を行なう STA (移動端末

局)と、前記STAからの前記公開鍵認証要求あるいは前記公開鍵再認証要求が妥当である場合には前記STAの認証を行う前記APと、を備えることを特徴とする無線LANシステムにおける認証装置。

【請求項10】 前記AP情報管理テーブルは、前記STAが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るAPのMACアドレスを最新認証完了実績順に保持することを特徴とする請求項9に記載の無線LANシステムにおける認証装置。

【請求項11】 前記APは、自らの秘密鍵であるAP秘密鍵と、前記AP秘密鍵に対応する公開鍵であるところのAP公開鍵と、前記AP公開鍵を付した自らのユーザ証明書であるところのAPユーザ証明書とを保持し、前記STAは、自らの秘密鍵であるSTA秘密鍵と、前記STA秘密鍵に対応する公開鍵であるところのSTA公開鍵と、前記STA公開鍵を付した自らのユーザ証明書であるところのSTAユーザ証明書とを保持している、ことを特徴とする請求項9或いは請求項10の何れか1項に記載の無線LANシステムにおける認証装置。

【請求項12】 前記STAが前記APに対して前記公開鍵認証要求を行う場合には、前記STAから前記APに対して認証要求を行い、前記認証要求を受信した前記APから前記STAに対して前記APユーザ証明書を送信し、前記APユーザ証明書を受信した前記STAが、前記APユーザ証明書を検証した後に前記APユーザ証明書に添付された前記AP公開鍵を用いて前記STAユーザ証明書を暗号化して暗号化STAユーザ証明書を作成し、前記暗号化STAユーザ証明書を前記APに対して送信し、前記暗号化STAユーザ証明書を受信した前記APが、前記暗号化STAユーザ証明書を前記AP秘密鍵で復号化して前記STAユーザ証明書を再生し、前記STAユーザ証明書を検証した後に前記STAユーザ証明書に添付された前記STA公開鍵を用いて前記APが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記STAに送信して認証許可を通知し、前記暗号化共通鍵を受信した前記STAが、前記暗号化共通鍵を前記STA秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする請求項11に記載の無線LANシステムにおける認証装置。

【請求項13】 前記STAが前記APに対して前記公開鍵認証要求を行う際に送受信されるMACフレーム内のフレームボディ部のAlgorithm Numberの値は、「0」又は「1」でない任意の数「n」である、ことを特徴とする請求項12に記載の無線LANシステムにおける認証装置。

【請求項14】 前記APは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記APが過去に認証許可を通知した実績の有る前記STAのMACアドレスと、該STAの前記STA公開鍵と、前記APが該STA

Aの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする請求項13に記載の無線LANシステムにおける認証装置。

【請求項15】 前記STAが前記APに対して前記公開鍵再認証要求を行う場合には、前記STAから前記APに対して再認証要求を行い、前記再認証要求を受信した前記APが、前記公開鍵再認証要求を送信した前記STAのMACアドレスが前記APの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記STAのMACアドレスが前記公開鍵管理テーブルに存在し、かつ、該MACアドレスに対応する公開鍵であるところの前記STA公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記APは、当該STAに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記STA公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記STAに送信して認証許可を通知し、前記暗号化新共通鍵を受信した前記STAが、前記暗号化新共通鍵を前記STA秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする請求項14に記載の無線LANシステムにおける認証装置。

【請求項16】 前記STAが前記APに対して前記公開鍵再認証要求を行う際に送受信されるMACフレーム内のフレームボディ部のAlgorithm Numberの値は、「0」と「1」と「n」でない任意の数「m」である、ことを特徴とする請求項15に記載の無線LANシステムにおける認証装置。

【発明の詳細な説明】

30 【0001】

【発明の属する技術分野】 本発明は無線LANシステムにおける認証方法と認証装置に関し、特にデータを暗号化して無線通信する無線LANシステムにおいて、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配達と認証の同時実現を可能とする、無線LANシステムにおける認証方法と認証装置に関する。

【0002】

【従来の技術】 無線LAN (Local Area Network : ラン) システムにおいては、送受信するデータの秘匿性を保持するために、送受信するデータフレームの暗号化が必須の条件となってきている。

【0003】 無線LANシステムにおける暗号化方式については、これまで IEEE (Institute of Electrical and Electronics Engineers : 米国、電気／電子技術者協会) 802委員会を中心として標準化の検討が進められており、その標準仕様であるIEEE802.11においては、無線LANにおける無線区間の暗号化及び認証の方式の1つとして、Shared Key (共通鍵) 認証方式が採用されている。

50 【0004】 Shared Key方式においては、図1に示すよ

うな無線LANの基地局としてのAP (Access Point : アクセスポイント) 1と移動端末局としてのSTA (Station : ステーション) 2とが、通信相手毎に互いに保持することのできる1種類の共通鍵を使用する、又は1種類の共通鍵を保持していない場合には、両者共通の鍵情報として4種類の共通鍵を保持しておき、フレーム暗号化通信を行う際には4種類の共通鍵の中の1つの共通鍵を選択して使用するようになっている。しかし、暗号化用の鍵の配送方法に関しては、IEEE802.11には定義されておらず、実装依存となっている。

【0005】Shared Key方式における認証手順について、図10及び図11を参照して説明する。

【0006】図10は、Shared Key方式における認証手順を示す図であり、図11は、Shared Key方式の認証手順において送受信されるフレームフォーマットのフレームボディ部を示す図である。

【0007】図10において、AP1に対してShared Key方式による認証要求を行うSTA2は、AP1に対して認証フレーム1を送信する(ステップS1)。認証フレーム1のフレームボディ部は、図11の(1)認証フレーム1に示す形式となっており、Algorithm Number (アルゴリズム番号) 11-1-1を「1」とし、Transaction Sequence Number (トランザクションシーケンス番号) 11-1-2を「1」としたフレームとなっている。なお、Shared Key方式における認証時には、Algorithm Number 11-1-1~11-4-1は常に「1」であると定義されている。

【0008】ステップS1でSTA2から認証要求を受信したAP1は、認証フレーム2を用いてChallenge Text (チャレンジテキスト) というランダムなビット列をSTA2に対して送信する(ステップS2)。認証フレーム2は、図11の(2)認証フレーム2に示す形式となっており、Algorithm Number 11-2-1は前述の通り「1」であり、Transaction Sequence Number 11-2-2は「2」で、Challenge Text element (チャレンジテキストエレメント) 11-2-4にChallenge Text を挿入したフレームとなっている。

【0009】ステップS2でAP1から認証フレーム2を受信したSTA2は、AP1から受信したChallenge Textと、該Challenge Textに対するCRC32(Cyclic Redundancy Code 32bits)算出結果に相当するICV (Integrity Check Value : インTEGRITY CHECK VALUE) に対して、共通鍵の1つで暗号化を行う(ステップS3)。そして、暗号化したChallenge TextとICVを、使用した共通鍵の鍵情報であるIV (Initialization Vector : イニシャライゼイション・ベクター)と共に、認証フレーム3を用いてAP1に対して送信する(ステップS4)。認証フレーム3は、図11の(3)認証フレーム3に示す形式となっており、Algorithm Number 11-3-1は前述の通り「1」であり、Transaction Sequen-

ce Number 11-3-2は「3」で、IV11-3-3、Challenge Text element (暗号化したChallenge Text) 11-3-4、ICV 11-3-5を付加したフレームとなっている。

【0010】ステップS4で認証フレーム3を受信したAP1は、受信フレーム内鍵情報 (IV11-3-3) からそれに対応する共通鍵を用いて受信フレームの暗号化部を復号化し、受信フレーム内ICV (ICV 11-3-5) と復号結果から算出したICVの一一致と、復号結果から得られる平文とステップS2で送信したChallenge Textとの一致を確認した場合には(ステップS5で一致を確認した場合)、認証フレーム4をSTA2に対して送信して認証完了を通知する(ステップS6)。認証フレーム4は、図11の(4)認証フレーム4に示す形式となっており、Algorithm Number 11-4-1は前述の通り「1」であり、Transaction Sequence Number 11-4-2は「4」で、Status Code (ステータスコード) 11-4-9を付加したフレームとなっている。なお、図11に示したStatus Code 11-1-9、Status Code 11-2-9、Status Code 11-3-9及びStatus Code 11-4-9は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【0011】以上の動作により、Shared Key方式における認証手順が終了し、以後、STA2とAP1間で共通鍵を用いたフレーム暗号化通信が行われるようになっている。

【0012】Shared Key方式における認証と鍵配送の方法には、様々な手法が多数提案されており、例えばその1つとして、通信を行う当事者以外の第三者(例えは鍵管理サーバ)を介在させる手法や、他の1つとして、通信を行う当事者間でのみ秘密情報の交換を行う手法がある。前者の一例としては、特開2001-111544号公報記載の「無線LANシステムにおける認証方法と認証装置」が知られており、この公報では、認証サーバと、何らかの方法で予め配布し保持させた共通鍵を用いて、暗号化認証を行う技術が記載されている。また、後者の一例としては、特開平11-191761号公報記載の「相互認証方法及びその装置」が知られており、この公報では、Diffie-Hellmanの鍵配送アルゴリズムを用いて公開鍵の正当性を確認する技術が記載されている。

【0013】

【発明が解決しようとする課題】第1の例として上述した鍵管理サーバを利用したシステムでは、予め移動端末局の情報を鍵管理サーバに登録しておくものであり、鍵配送手順と認証手順が分離されることにより、暗号化を伴う認証手順が複雑なものとなるという欠点を有している。

【0014】また、第2の例として上述した鍵配送アルゴリズムを用いた認証手順においては、通信を行った当事者間でのみ秘匿性を保持した鍵配送と認証を同時にう

ことが可能となるが、その認証手順が複雑となり演算に多くの時間を要するものとなっており、無線伝播環境の問題などによって通信が絶たれた際の認証解除時における再度の認証手順実行時にも、初回の認証時と同一手順を踏むこととなり、本来のデータ通信以外のオーバーヘッドトラヒックを増大させてしまうという欠点を有している。

【0015】本発明は上述した事情を改善するためになされたものであり、本発明の目的は、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配達と認証手順の同時実現を可能とすると共に、初回の認証を完了したSTA（移動端末局）に関しては、認証解除後の同一AP（基地局）に対する2回目以降の認証手順の簡略化を実現可能とする、無線LANシステムにおける認証方法と認証装置を提供することにある。

【0016】

【課題を解決するための手段】本発明の無線LANシステムにおける認証方法は、無線LANシステムにおける認証方法において、STA（移動端末局）は、無線通信を行おうとするAP（基地局）のMACアドレスが前記STAの保持するAP情報管理テーブル内に存在するか否かを検索し、前記MACアドレスが前記AP情報管理テーブル内に存在しない場合には、前記STAは前記APに対して公開鍵認証要求を行い、前記APは前記公開鍵認証要求が妥当である場合には前記STAの認証を行い、前記MACアドレスが前記AP情報管理テーブル内に存在する場合には、前記STAは前記APに対して公開鍵再認証要求を行い、前記APは前記公開鍵再認証要求が妥当である場合には前記STAの認証を行う、ことを特徴とする。

【0017】また、前記AP情報管理テーブルは、前記STAが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るAPのMACアドレスを最新認証完了実績順に保持することを特徴とする。

【0018】さらに、前記APは、自らの秘密鍵であるAP秘密鍵と、前記AP秘密鍵に対応する公開鍵であるところのAP公開鍵と、前記AP公開鍵を付した自らのユーザ証明書であるところのAPユーザ証明書とを保持し、前記STAは、自らの秘密鍵であるSTA秘密鍵と、前記STA秘密鍵に対応する公開鍵であるところのSTA公開鍵と、前記STA公開鍵を付した自らのユーザ証明書であるところのSTAユーザ証明書とを保持している、ことを特徴とする。

【0019】また、前記STAが前記APに対して前記公開鍵認証要求を行うステップは、公開鍵認証手順によって構成され、前記公開鍵認証手順は、前記STAから前記APに対して認証要求を行うステップと、前記認証要求を受信した前記APから前記STAに対して前記APユーザ証明書を送信するステップと、前記APユーザ証明書を受信した前記STAが、前記APユーザ証明書

を検証した後に前記APユーザ証明書に添付された前記AP公開鍵を用いて前記STAユーザ証明書を暗号化して暗号化STAユーザ証明書を作成し、前記暗号化STAユーザ証明書を前記APに対して送信するステップと、前記暗号化STAユーザ証明書を受信した前記APが、前記暗号化STAユーザ証明書を前記AP秘密鍵で復号化して前記STAユーザ証明書を再生し、前記STAユーザ証明書を検証した後に前記STAユーザ証明書に添付された前記STA公開鍵を用いて前記APが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記STAに送信して認証許可を通知するステップとから構成され、前記暗号化共通鍵を受信した前記STAが、前記暗号化共通鍵を前記STA秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用する、ことを特徴とする。

【0020】さらに、前記STAが前記APに対して前記公開鍵認証要求を行う際に送受信されるMACフレーム内のフレームボディ部のAlgorithm Numberの値は、「0」又は「1」でない任意の数「n」である、ことを特徴とする。

【0021】また、前記APは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記APが過去に認証許可を通知した実績の有る前記STAのMACアドレスと、該STAの前記STA公開鍵と、前記APが該STAの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする。

【0022】さらに、前記STAが前記APに対して前記公開鍵再認証要求を行うステップは、公開鍵再認証手順によって構成され、前記公開鍵再認証手順は、前記STAから前記APに対して再認証要求を行うステップ

と、前記再認証要求を受信した前記APが、前記公開鍵再認証要求を送信した前記STAのMACアドレスが前記APの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記STAのMACアドレスが前記公開鍵管理テーブルに存在し、かつ、該MACアドレスに対応する公開鍵であるところの前記STA公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記APは、当該STAに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵

を前記STA公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記STAに送信して認証許可を通知するステップとから構成され、前記暗号化新共通鍵を受信した前記STAが、前記暗号化新共通鍵を前記STA秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用する、ことを特徴とする。

【0023】また、前記STAが前記APに対して前記公開鍵再認証要求を行う際に送受信されるMACフレーム内のフレームボディ部のAlgorithm Numberの値は、「0」と「1」と「n」でない任意の数「m」である、

ことを特徴とする。

【0024】本発明の無線LANシステムにおける認証装置は、無線LANシステムにおける認証装置において、無線通信を行おうとするAP(基地局)のMACアドレスが自身の保持するAP情報管理テーブル内に存在するか否かを検索し、前記MACアドレスが前記AP情報管理テーブル内に存在しない場合には、前記APに対して公開鍵認証要求を行い、前記MACアドレスが前記AP情報管理テーブル内に存在する場合には、前記APに対して公開鍵再認証要求を行うSTA(移動端末局)と、前記STAからの前記公開鍵認証要求あるいは前記公開鍵再認証要求が妥当である場合には前記STAの認証を行う前記APと、を備えることを特徴とする。

【0025】また、前記AP情報管理テーブルは、前記STAが前記公開鍵認証要求を行って該公開鍵認証の完了実績の有るAPのMACアドレスを最新認証完了実績順に保持することを特徴とする。

【0026】さらに、前記APは、自らの秘密鍵であるAP秘密鍵と、前記AP秘密鍵に対応する公開鍵であるところのAP公開鍵と、前記AP公開鍵を付した自らのユーザ証明書であるところのAPユーザ証明書とを保持し、前記STAは、自らの秘密鍵であるSTA秘密鍵と、前記STA秘密鍵に対応する公開鍵であるところのSTA公開鍵と、前記STA公開鍵を付した自らのユーザ証明書であるところのSTAユーザ証明書とを保持している、ことを特徴とする。

【0027】また、前記STAが前記APに対して前記公開鍵認証要求を行う場合には、前記STAから前記APに対して認証要求を行い、前記認証要求を受信した前記APから前記STAに対して前記APユーザ証明書を送信し、前記APユーザ証明書を受信した前記STAが、前記APユーザ証明書を検証した後に前記APユーザ証明書に添付された前記AP公開鍵を用いて前記STAユーザ証明書を暗号化して暗号化STAユーザ証明書を作成し、前記暗号化STAユーザ証明書を前記APに対して送信し、前記暗号化STAユーザ証明書を受信した前記APが、前記暗号化STAユーザ証明書を前記AP秘密鍵で復号化して前記STAユーザ証明書を再生し、前記STAユーザ証明書を検証した後に前記STAユーザ証明書に添付された前記STA公開鍵を用いて前記APが生成した共通鍵を暗号化して暗号化共通鍵を作成し、前記暗号化共通鍵を前記STAに送信して認証許可を通知し、前記暗号化共通鍵を受信した前記STAが、前記暗号化共通鍵を前記STA秘密鍵で復号化して前記共通鍵を再生し、以降のフレーム暗号化通信に該共通鍵を使用することを特徴とする。

【0028】さらに、前記STAが前記APに対して前記公開鍵認証要求を行う際に送受信されるMACフレーム内のフレームボディ部のAlgorithm Numberの値は、「0」又は「1」でない任意の数「n」である、ことを

特徴とする。

【0029】また、前記APは公開鍵管理テーブルを保持し、前記公開鍵管理テーブルは前記APが過去に認証許可を通知した実績の有る前記STAのMACアドレスと、該STAの前記STA公開鍵と、前記APが該STAの認証許可時に生成し発行した共通鍵とを、最新認証許可順に保持する、ことを特徴とする。

【0030】さらに、前記STAが前記APに対して前記公開鍵再認証要求を行う場合には、前記STAから前記APに対して再認証要求を行い、前記再認証要求を受信した前記APが、前記公開鍵再認証要求を送信した前記STAのMACアドレスが前記APの保持する前記公開鍵管理テーブル内に存在するか検索し、検索した結果、前記STAのMACアドレスが前記公開鍵管理テーブルに存在し、かつ、該MACアドレスに対応する公開鍵であるところの前記STA公開鍵を前記公開鍵管理テーブル内に保持していることを確認した場合には、前記APは、当該STAに対して指定する新たな共通鍵である新共通鍵を生成し、該新共通鍵を前記STA公開鍵で暗号化して暗号化新共通鍵を生成し、該暗号化新共通鍵を前記STAに送信して認証許可を通知し、前記暗号化新共通鍵を受信した前記STAが、前記暗号化新共通鍵を前記STA秘密鍵で復号化して前記新共通鍵を再生し、以降のフレーム暗号化通信に該新共通鍵を使用することを特徴とする。

【0031】また、前記STAが前記APに対して前記公開鍵再認証要求を行う際に送受信されるMACフレーム内のフレームボディ部のAlgorithm Numberの値は、「0」と「1」と「n」でない任意の数「m」である、ことを特徴とする。

【0032】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0033】図1は本発明の無線LANシステムにおける認証装置の一実施形態を示すブロック図である。

【0034】図1に示す本実施の形態は、無線LANの基地局としてのAP(Access Point: アクセスポイント)1と、AP1に帰属する移動端末局としての複数のSTA(Station:ステーション)2(STA2-1、STA2-k)とから構成されている。図1に示す実施の形態は、IEEE802.11で定義するところのInfrastructure(インフラストラクチャ)方式であり、このような無線LANネットワークの最小単位をBSS(Basic Service Set: 基本サービス・セット)4と言う。

【0035】BSS4内におけるAP1は、各STA2がAP1に同期するための情報を含むBeacon(ビーコン)フレームを、周期的にBSS4内にプロードキャスト送信し、当該Beaconフレームを受信したBSS4内の各STA2は、通信開始時にAP1に対して認証要求を行い、AP1により認証許可を受けた後、AP1への帰

属処理を完了することにより、AP1との通信を行うことが可能となる。また、Infrastructure方式におけるBSS4内の各STA2は、STA2間通信時においてもAP1を介した通信を行う。

【0036】また、図1におけるAP1は(portal)となっているが、Portalとは、IEEE802.11以外のLANプロトコルとのプロトコル変換機能をAP1に付加したことをしており、基地局としてのAP1とEthernet (登録商標) (イーサネット (登録商標)) 5などの有線LANとの接続を可能にした基地局であることを示している。

【0037】なお、図1に示した実施の形態は、IEEE802.11に準拠したものであるが、本実施の形態においては無線区間の暗号化及び認証の方式として、Shared Key方式（共通鍵認証方式）とは異なり、主として秘密鍵と公開鍵を用いた認証方式を採用している。従って、Shared Key方式と区別するために、本実施形態における認証方式を公開鍵認証方式と便宜的に呼ぶこととする。

【0038】次に、図2を参照して、AP1とSTA2の詳細構成について説明する。

【0039】図2は、APとSTAの一例を示す詳細ブロック図である。

【0040】図2において、上段のブロック図がAP1であり、下段のブロック図がSTA2である。

【0041】AP1は、図2に示す無線LANカード19-1と上位レイヤとのインターフェースであるところの上位レイヤインターフェース17-1を介して、TCP/IP (Transport Control Protocol/Internet Protocol) や各種アプリケーションなどの上位プロトコル処理を、基地局端末本体18にて実現するものであり、STA2は、図2に示す無線LANカード19-2と上位レイヤとのインターフェースであるところの上位レイヤインターフェース17-2を介して、AP1と同様な上位プロトコル処理を、ノート型パーソナルコンピュータなどの移動端末本体20によって実現するものである。

【0042】図2に示す無線LANカード19-1と無線LANカード19-2は、同一の構成を備える。従って、無線LANカード19において同一の構成要素に対応するものは、同一の参照数字または符号を付しておくものとする。

【0043】図2に示す無線LANカード19 (19-1及び19-2) は、無線区間でのフレーム送受信を行う無線機部12と、変復調処理を行うIEEE802.11 PHY (Physical Layer: 物理層) プロトコル処理部13と、MAC (Medium Access Control : 媒体アクセス制御) 層でのアクセス制御を行うIEEE802.11 MACプロトコル処理部14と、MAC層での認証処理などの上位レイヤ処理を、内蔵するCPUとメモリ16によって実現する上位レイヤ処理部15と、上位レイヤ処理部15が使用するメモリ16とから構成されている。

【0044】次に、図3を参照して、STA2がAP1に対して認証を要求する際に、STA2とAP1間で送受信されるMACフレームについて説明する。

【0045】図3は、認証要求時にAPとSTA間で送受信されるMACフレームの構成を説明する図である。

【0046】STA2のAP1に対する認証要求時には、図3に示すIEEE802.11のMACフレームフォーマットに従うMACフレーム30-1が、AP1とSTA2間で交換され、MACフレーム30-1は、MAC Header

10 (MACヘッダー) 30-2と、FrameBody (フレームボディ) 30-3とFCS (Frame Check Sequence: フレームチェックシーケンス) 30-4とから構成されている。

【0047】そして、Infrastructure方式におけるMAC Header 30-2は、各種フレームタイプや制御情報を示すFrame Control (フレームコントロール) 30-11のフィールドと、送信先がビジーである場合に送信待機を行うための時間を定義するDuration (デュレーション) 30-12のフィールドと、フレーム送信先アドレスを示すDA (Destination Address : 送信先アドレス) 30-13のフィールドと、フレームの送信元アドレスを示すSA (Source Address : 送信元アドレス) 30-14のフィールドと、BSS4の識別情報を示すBSSID 30-15のフィールドと、フレーム送信順を示すSequence Control (シーケンスコントロール) 30-16のフィールドから構成される。

【0048】フレーム送信時、図2に示すIEEE802.11 MACプロトコル処理部14では、上位レイヤ処理部15からの送信要求フレームを、図3に示すFrameBody 30-3に入れてカプセル化し、送信要求情報から作成したMAC Header 30-2をFrameBody 30-3の前に付加し、当該MAC Header 30-2とFrameBody 30-3に対するCRC32 (Cyclic Redundancy Code 32bits) 算出結果を、FCS 30-4としてFrameBody 30-3の後に付加することにより、図3に示すようなIEEE802.11 MACプロトコルに従うMACフレーム30-1への変換を行う。続いて図2に示すIEEE802.11 PHYプロトコル処理部13では、当該MACフレーム30-1に対する変調処理を行い、無線機部12を経て当該MACフレーム30-1を40 空間に送出することにより、送信処理が完了する。

【0049】フレーム受信時、図2に示すIEEE802.11 MACプロトコル処理部14では、無線機部12を経てIEEE802.11 PHYプロトコル処理部13にて復調処理を行った結果として受信したMACフレーム30-1に対してCRC32の計算を行い、受信フレーム内のFCS 30-4の値とCRC32算出結果とが一致する場合には、MAC Header 30-2の内容の解析と受信フレームに対する処理を行い、FrameBody 30-3の部分を上位レイヤ処理部15へ通知する。

50 【0050】次に、図4及び図5を参照して、本実施形

態の重要な構成要素としての公開鍵管理テーブル及びAP情報管理テーブルについて説明する。

【0051】図4は、APが保持する公開鍵管理テーブルを説明する図であり、図5は、STAが保持するAP情報管理テーブルを説明する図である。

【0052】AP1は、図4に示す公開鍵管理テーブル40を、図2に示す無線LANカード19-1のメモリ16内に保持している。公開鍵管理テーブル40は、AP1が過去に本発明の公開鍵認証において認証許可を行った実績の有るSTA2のMAC層の物理アドレスであるところのMACアドレスを保持するSTA Mac Address(STAのMACアドレス)40-1の欄と、当該STA2の公開鍵を保持するPublic Key(パブリックキー)40-2の欄と、AP1が認証許可時に当該STA2に対して発行した共通鍵を保持するShared Key(シェアードキー)40-3の欄とから構成されている。そして、AP1は公開鍵管理テーブル40の各行を、STA2の最新認証許可順に登録する。

【0053】STA2は、図5に示すAP情報管理テーブル50を、図2に示す無線LANカード19-2のメモリ16内に保持している。AP情報管理テーブル50は、STA2が本発明の公開鍵認証を要求して該公開鍵認証の完了実績の有るAP1のMACアドレスを保持するAP MAC Address(APのMACアドレス)50-1の欄から構成されており、STA2はAP情報管理テーブル50の各行を、AP1の最新認証完了実績順に登録する。

【0054】AP1は、図4にて説明した公開鍵管理テーブル40への情報登録時には、登録済みのSTA MAC address 40-1の検索を行い、既に登録済みの同一MACアドレスが存在する場合には、登録内容の情報更新と共に公開鍵管理テーブル40の先頭の行へ当該情報を移動する。また、本発明の公開鍵認証完了後のフレーム暗号化通信の実施毎に、AP1は公開鍵管理テーブル40のSTA MAC address 40-1の検索を行い、通信相手のSTA2の管理情報を公開鍵管理テーブル40の先頭の行へ移動することにより、通信機会が新しい通信相手の管理情報ほど管理テーブル上位に位置付けることで、公開鍵管理テーブル40が限界登録数に達し、新規情報登録が不可能となった場合には、公開鍵管理テーブル40内で最も下位に位置する通信機会の最も古い通信相手の管理情報を削除することで対応する。

【0055】また、STA2はAP1と同様に、図5にて説明したAP情報管理テーブル50への情報登録時には、登録済みのAP MAC address 50-1の検索を行い、既に登録済みの同一MACアドレスが存在する場合には、登録内容の情報更新と共にAP情報管理テーブル50の先頭の行へ当該情報を移動する。また、本発明の公開鍵認証完了後のフレーム暗号化通信の実施毎に、STA2はAP情報管理テーブル50のAP MAC address 50

-1の検索を行い、通信相手のAP1の管理情報をAP情報管理テーブル50の先頭の行へ移動することにより、通信機会が新しい通信相手の管理情報ほど管理テーブル上位に位置付けることで、AP情報管理テーブル50が限界登録数に達し、新規情報登録が不可能となった場合には、AP情報管理テーブル50内で最も下位に位置する通信機会の最も古い通信相手の管理情報を削除することで対応する。

【0056】次に、図6、図7、図8、図9を参照して、本実施形態の動作について説明する。

【0057】本実施形態においては、図1に示した無線LANシステムの、基地局であるAP1と移動端末局であるSTA2は、共に、自らの秘密鍵とそれに対応する公開鍵、及び該公開鍵を添付したユーザ証明書を保持しているものとする。そして、当該ユーザ証明書は、認証機関に代表される第三者によって、公開鍵とその保有者(すなわち、AP1或いはSTA2)との関係、及び保有者自身の正当性を証明可能である、という条件を前提とするものとする。以下では、ユーザ証明書はデジタルユーザ証明書を意味するものとする。

【0058】図1におけるSTA2がAP1を介しての無線通信を行おうとする場合には、STA2は先ずAP1に対して、本発明の公開鍵認証要求を送信することから開始する。

【0059】STA2は公開鍵認証開始時に、認証要求先のAP1のMACアドレスを用いて図5に示したAP情報管理テーブル50内のAP MAC Address 50-1の検索を行い、AP情報管理テーブル50内に認証要求先AP1のMACアドレスが存在しない場合には、初回の認証要求として図6に示す公開鍵認証手順を行い、認証要求先AP1のMACアドレスが存在する場合には、過去に当該AP1との公開鍵認証の完了実績が有る場合であるため、再認証として、図8に示す公開鍵再認証手順を行う。

【0060】先ず、初回の認証要求としての公開鍵認証手順について、図6及び図7を参照して説明する。

【0061】図6は、公開鍵認証手順を示す図であり、図7は、公開鍵認証手順において送受信されるMACフレームのフレームボディ部(図3のFrameBody 30-3)を示す図である。

【0062】図6において、AP1に対して公開鍵認証手順による認証要求を行うSTA2は、AP1に対して認証フレーム61を送信する(ステップS61)。認証フレーム61のフレームボディ部は、図7の(1)認証フレーム61に示す形式となっており、Algorithm Number(アルゴリズム番号)70-1-1を「n」とし、Transaction Sequence Number(トランザクションシーケンス番号)70-1-2を「1」としたフレームとなっている。なお、公開鍵認証手順における認証時には、Algorithm Number 70-1-1～70-4-1は常に

「n」(nは「0」又は「1」でない任意の数)であるものと定義する。Algorithm Number 70-1-1~70-4-1を「n」とすることにより、Shared Key方式による認証手順と区別することが可能となる。

【0063】ステップS61でSTA2から公開鍵認証要求を受信したAP1は、認証フレーム62を用いてAP1の保持するユーザ証明書をSTA2に対して送信する(ステップS62)。認証フレーム62は、図7の(2)認証フレーム62に示す形式となっており、Algorithm Number 70-2-1は前述の通り「n」であり、Transaction Sequence Number 70-2-2は「2」で、APのユーザ証明書70-2-3にAP1の保持するユーザ証明書(ユーザ証明書に付随するAP1の公開鍵をも付したもの)を挿入したフレームとなっている。

【0064】ステップS62でAP1から認証フレーム62を受信したSTA2は、AP1から受信したAP1のユーザ証明書の内容を検証して、AP1のユーザ証明書の検証結果に問題の無いことを確認すると、AP1のユーザ証明書に添付された公開鍵を用いて、STA2の保持するユーザ証明書の暗号化を行う(ステップS63)。そして、暗号化したSTA2のユーザ証明書を、STA2のユーザ証明書に付随するSTA2の公開鍵と共に、認証フレーム63を用いてAP1に対して送信する(ステップS64)。認証フレーム63は、図7の(3)認証フレーム63に示す形式となっており、Algorithm Number 70-3-1は前述の通り「n」であり、Transaction Sequence Number 70-3-2は「3」で、APの公開鍵で暗号化したSTAのユーザ証明書70-3-3を付加したフレームとなっている。

【0065】ステップS64で認証フレーム63を受信したAP1は、APの公開鍵で暗号化したSTAのユーザ証明書70-3-3をAP1の秘密鍵で復号化して、STA2のユーザ証明書の内容を検証し、STA2のユーザ証明書の検証結果に問題の無いことを確認すると、次に今度は共通鍵を生成し、STA2のユーザ証明書に添付された公開鍵を用いて生成した共通鍵を暗号化する(ステップS65)。そして暗号化した共通鍵を、認証フレーム64を用いてSTA2に送信し、認証許可を通知する(ステップS66)。認証フレーム64は、図7の(4)認証フレーム64に示す形式となっており、Algorithm Number 70-4-1は前述の通り「n」であり、Transaction Sequence Number 70-4-2は「4」で、STAの公開鍵で暗号化した共通鍵70-4-3を付加したフレームとなっている。なお、図7に示したStatus Code 70-1-9、Status Code 70-2-9、Status Code 70-3-9及びStatus Code 70-4-9は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【0066】その後、ステップS66でAP1から認証フレーム64を受信したSTA2は、STAの公開鍵で暗

号化した共通鍵70-4-3をSTA2の秘密鍵で復号化して、AP1が生成した共通鍵を復元し、この後実際に行われる無線通信におけるフレーム暗号化に、該共通鍵を使用することとなる(ステップS67)。以上の動作により、公開鍵認証手順が終了となり、以後、STA2とAP1間でフレーム暗号化通信が行われることとなる。

【0067】次に、再認証が行われる際の公開鍵再認証手順について、図8及び図9を参照して説明する。

10 【0068】図8は、公開鍵再認証手順を示す図であり、図9は、公開鍵再認証手順において送受信されるMACフレームのフレームボディ部(図3のFrameBody 30-3)を示す図である。

【0069】図8において、認証要求先のAP1に対して過去に公開鍵認証完了実績のあるSTA2は、公開鍵再認証要求としてAP1に対して認証フレーム81を送信する(ステップS81)。認証フレーム81のフレームボディ部は、図9の(1)認証フレーム81に示す形式となっており、Algorithm Number(アルゴリズム番号)90-1-1を「m」とし、Transaction Sequence Number(トランザクションシーケンス番号)90-1-2を「1」としたフレームとなっている。なお、公開鍵再認証手順における認証時には、Algorithm Number 90-1-1~90-2-1は常に「m」(mは「0」と「1」と「n」でない任意の数)であるものと定義する。Algorithm Number 90-1-1~90-2-1を「m」とすることにより、図6に示した公開鍵認証手順と区別することが可能となる。

【0070】ステップS81でSTA2から公開鍵再認証要求を受信したAP1は、AP1が保持している図4に示した公開鍵管理テーブル40において、公開鍵再認証要求を送信したSTA2のMACアドレスがSTA Mac Address 40-1に存在するか検索を行う(ステップS82)。

そして、検索が成功し、かつ、それに対応する公開鍵をPublic Key 40-2の欄に保持していることを確認した場合には、AP1は当該STA2に対して指定する共通鍵を新たに生成し、この新共通鍵を公開鍵管理テーブル40のPublic Key 40-2から取得した公開鍵(当該STA2の公開鍵)を用いて暗号化する(ステップS83)。そして、暗号化した新共通鍵を、認証フレーム82を用いてSTA2に送信する(ステップS84)。

認証フレーム82は、図9の(2)認証フレーム82に示す形式となっており、Algorithm Number 90-2-1は前述の通り「m」であり、Transaction Sequence Number 90-2-2は「2」で、STAの公開鍵で暗号化した新共通鍵90-2-3を付加したフレームとなっている。なお、図9に示したStatus Code 90-1-9及びStatus Code 90-2-9は、フレーム受信成功の可否などを通信相手に通知するための情報フィールドである。

【0071】その後、ステップS84でAP1から認証フレームS82を受信したSTA2は、STAの公開鍵で暗号化した新共通鍵90-2-3をSTA2の保持する秘密鍵で復号化して、AP1が新たに生成した新共通鍵を復元し、この後実際に行われる無線通信におけるフレーム暗号化に、該新共通鍵を使用することとなる(ステップS85)。以上の動作により、公開鍵再認証手順が終了となり、以後、STA2とAP1間でフレーム暗号化通信が行われることとなる。

【0072】以上、本発明の第1の実施形態について詳細に説明した。第1の実施形態においては、AP1とSTA2が共に自らの秘密鍵とそれに対応する公開鍵、及び公開鍵を添付したユーザ証明書を保持し、当該ユーザ証明書は認証機関に代表される第三者によって公開鍵とその保有者との関係及び保有者自身の正当性を証明可能であるという条件のもとで、STA2がAP1に対して公開鍵認証要求を行い、AP1から認証許可を得るまでには、図6に示す公開鍵の交換手順が発生するが、本発明に基づき、AP1とSTA2が認証完了実績のある相手の公開鍵情報を認証解除後も保持し続けることにより、2回目以降の認証要求時において図8に示す公開鍵再認証手順を用いることにより、初回の認証手順で行ったAP1とSTA2間での公開鍵交換手順を省略することで、認証処理手順の簡略化が可能となる、という効果を有している。

【0073】また、図6に示す初回の公開鍵認証手順においてユーザ証明書を用いることにより、AP1はSTA2の公開鍵とその保有者であるSTA2の正当性とを確認した上で認証許可後にSTA2の公開鍵情報を保持することから、当該STA2のMACアドレスを使用した成りすましによる再認証要求が発生した場合には、図8に示す公開鍵再認証手順を行うAP1は、STA2に対して送信する共通鍵を正当なSTA2のみが保持する秘密鍵に対応した公開鍵によって暗号化するため、成りすましによる再認証要求元STAはこれを復号化し共通鍵を取得することができず、従って本発明によって不正なSTAによる成りすましを防ぐことが可能となる、という効果を有している。

【0074】次に、本発明の第2の実施形態について説明する。

【0075】第2の実施形態は、複数のAP(基地局)による複数のBSS(基本サービス・セット)が存在し、且つ各BSS同士が有線又は無線で接続される複合ネットワーク上において、各APに帰属中のSTA(移動端末局)に関する公開鍵管理情報(具体的には、図4に示した公開鍵管理テーブル40)を、複合ネットワーク内における共有情報とする構成とした無線LANシステムである。複合ネットワーク内における共有情報とする構成は、例えば、複数のAPを統括する上位APを配設し、上位APが公開鍵管理情報を一括して保持してお

き、各APは必要時に上位APに対する登録あるいは問い合わせを行い、その回答を上位APから得る構成である。このような構成とすることにより、任意APに帰属中のSTAが、BSSの移動により他のAPへ初回の公開鍵認証を行う際にも、本発明による公開鍵再認証手順を実施することにより認証処理手順の簡略化が可能となる、という効果を有するものとなる。

【0076】次に、本発明の第3の実施形態について説明する。

- 10 【0077】第3の実施形態は、IEEE802.11で定義するところのIndependent(インディペンデント:独立)方式の無線LANシステムに第1の実施形態の本発明を適用する構成である。Independent方式では、IBSS(Independent BSS:インディペンデントBSS)内に複数のSTAだけが存在し、APは存在しない。そして、IBSS内におけるSTA間での公開鍵認証時において、本発明の第1の実施形態に基づき、公開鍵認証要求を受信したSTAが認証要求元STAの公開鍵管理情報(具体的には、図4に示した公開鍵管理テーブル40)を保持し続ける構成としたものである。このような構成とすることにより、2回目以降の公開鍵再認証処理手順の簡略化が可能となる、という効果を有するものとなる。

- 20 【0078】なお、本発明の第1、第2及び第3の実施形態において、認証許可を行うBSS内APやIBSS内STAが保持する認証要求元STAに関する公開鍵管理情報と共に、ユーザ証明書に基づく有効期限情報を導入することによって、公開鍵管理情報の保持期限を持たせる構成とすることにより、有効期限切れユーザ証明書の継続使用を防ぐことが可能となる。

- 30 【0079】
【発明の効果】以上説明したように、本発明の無線LANシステムにおける認証方法と認証装置は、無線通信を行う当事者間でのみ秘匿性を保持した暗号用の鍵配達と認証手順の同時実現を可能とすることができるので、初回の認証を完了したSTA(移動端末局)に関しては、認証解除後の同一AP(基地局)に対する2回目以降の認証手順の簡略化を実現可能とする、という効果を有している。

40 【図面の簡単な説明】

【図1】本発明の無線LANシステムにおける認証装置の一実施形態を示すブロック図である。

【図2】APとSTAの一例を示す詳細ブロック図である。

【図3】認証要求時にAPとSTA間で送受信されるMACフレームの構成を説明する図である。

【図4】APが保持する公開鍵管理テーブルを説明する図である。

- 50 【図5】STAが保持するAP情報管理テーブルを説明する図である。

【図6】公開鍵認証手順を示す図である。

【図7】公開鍵認証手順において送受信されるMACフレームのフレームボディ部を示す図である。

【図8】公開鍵再認証手順を示す図である。

【図9】公開鍵再認証手順において送受信されるMACフレームのフレームボディ部を示す図である。

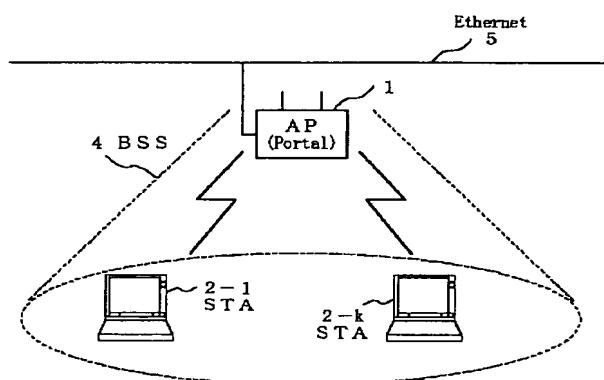
【図10】Shared Key方式における認証手順を示す図である。

【図11】Shared Key方式の認証手順において送受信されるフレームフォーマットのフレームボディ部を示す図である。

【符号の説明】

1 A P

【図1】



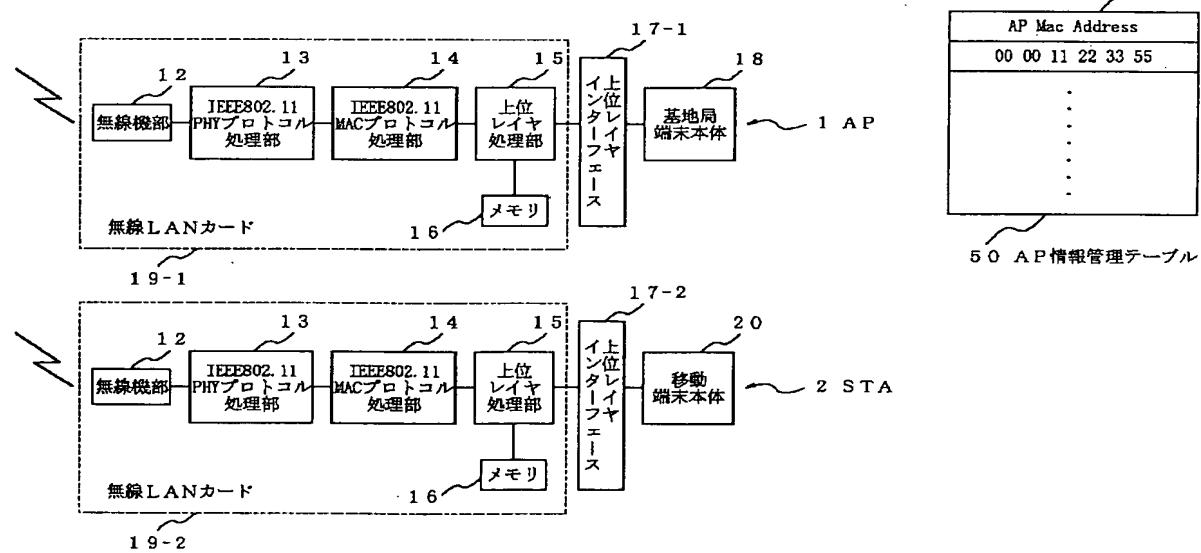
【図4】

4 0 - 1	4 0 - 2	4 0 - 3
STA Mac Address	Public Key	Shared Key
00 00 11 22 33 44	Key Data	Key Data
⋮	⋮	⋮
⋮	⋮	⋮
⋮	⋮	⋮

4 0 公開鍵管理テーブル

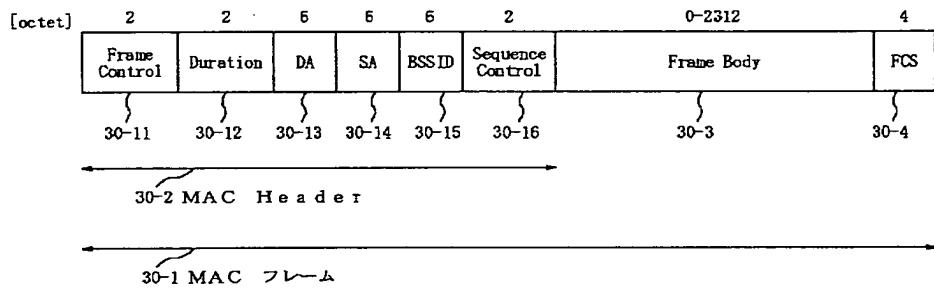
【図5】

【図2】

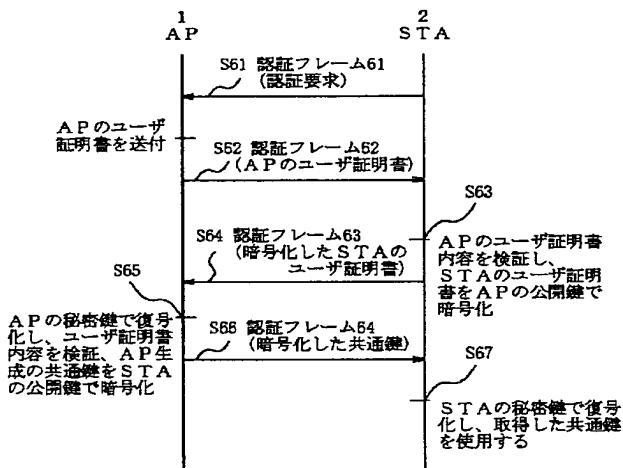


20
2 STA
4 BSS
5 Ethernet (イーサネット)
12 無線機部
13 IEEE802.11 PHYプロトコル処理部
14 IEEE802.11 MACプロトコル処理部
15 上位レイヤ処理部
16 メモリ
17 上位レイヤインターフェース
18 基地局端末本体
19 Shared Key
20 移動端末本体

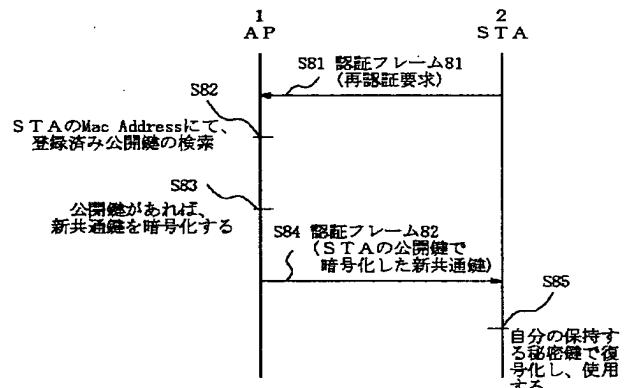
【図3】



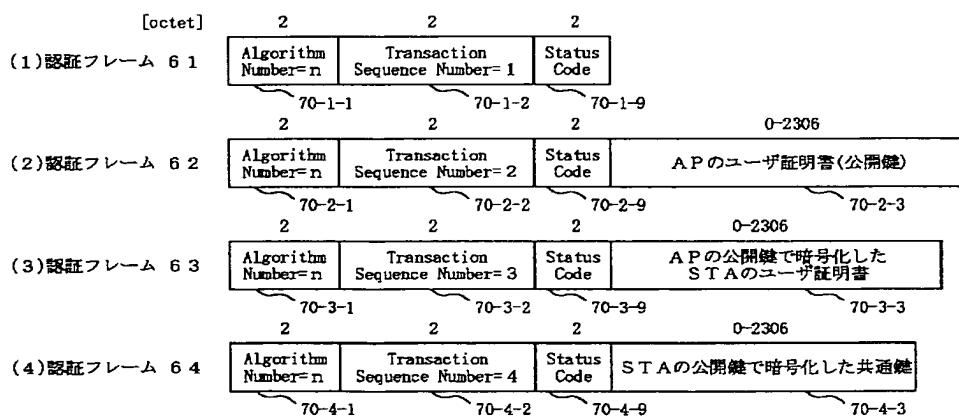
【図6】



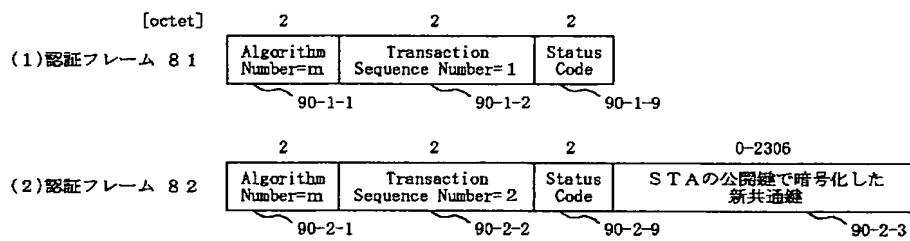
【図8】



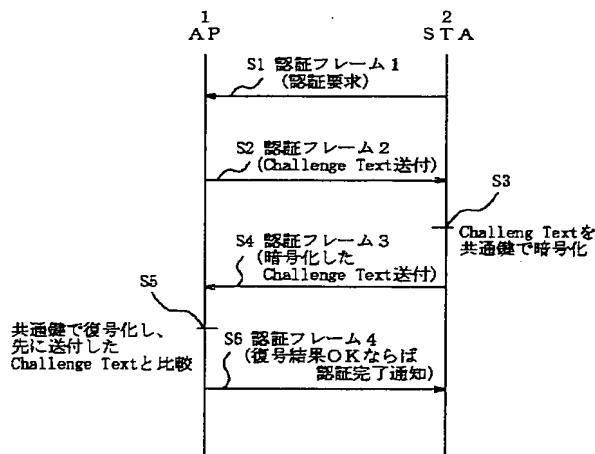
【図7】



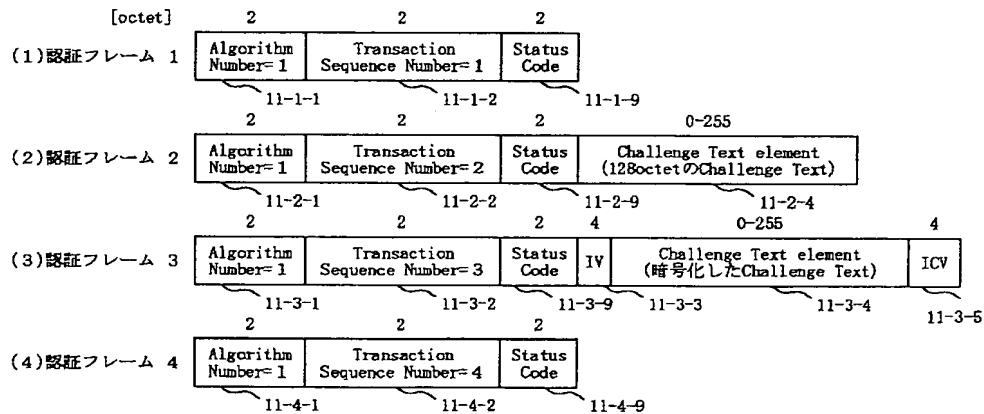
【図9】



【図10】



【図11】



THIS PAGE BLANK (USPTO)